AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Black Samsung Cell Phone IMEI # 354142110521996

Case No. 20-MJ-370-JFJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 846	**Drugs Conspiracy**
21 U.S.C. § 841(a)(1)	**Possession With Intent to Distribute Methamphetamine**

The application is based on these facts:

See Affidavit of TFO William Mackenzie, DEA, attached hereto.

☑ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

TFO William Mackenzie, DEA
Printed name and title

by phone. JJ

Sworn to before me ~~and signed in my presence~~.

Date: 10-20-20

Judge's signature

City and state: Tulsa, OK

U.S. Magistrate Jodi F. Jayne
Printed name and title

RMR/tc

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

William R. Mackenzie, being duly sworn under oath, states as follows:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices (Attachment A)—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been deputized as a Task Force Officer with the Drug Enforcement Administration (DEA) and I am presently assigned to the Tulsa, Oklahoma office. I am also a police officer for the Tulsa Police Department and have been so for over nineteen years. I have a Bachelor's Degree in Criminal Justice from East Central University. Since becoming a Narcotics Detective with the Tulsa Police Department, I have participated in wire and physical surveillance, surveillance of undercover transactions, the introduction of undercover agents, the execution of search warrants, debriefings of informants and reviews of taped conversations and drug records. Through my training, education and experience, I have become familiar with the manner in which illegal drugs are transported, stored, and distributed and the methods of payment for such drugs. I have been the primary investigator in more than five complex conspiracy cases prosecuted within the federal justice system.

3. I have trained other narcotic detectives within the Tulsa Police Department's Special Investigations Division. I have completed the Oklahoma State

Bureau of Investigations Clandestine Laboratory Basic Safety Certification and Clandestine Laboratory Site Safety Officer courses presented by Network Environmental Systems. I have completed the Drug Enforcement Administration Basic Narcotics Investigator School. I have completed an Advanced Undercover Narcotics School. I have completed a Southwest Border Intelligence school and an Outlaw Motorcycle Gang school presented by the Association of Oklahoma Narcotic Enforcers. I have completed a Complex Conspiracies school presented by the Midwest Counterdrug Training Center. I have completed a Communication Exploitation Training presented by the Drug Enforcement Administration Special Operations Division. I have received formal training in narcotics investigations from the Tulsa Police Academy, as well as informal training received from more experienced officers.

4. I have participated in over 500 drug related criminal investigations. I have authored federal Title III affidavits and both state and federal search warrants. I have participated in several Title III investigations, purchased narcotics in an undercover capacity on numerous occasions, and executed controlled deliveries of narcotics. I have interviewed hundreds of defendants involved in the use, manufacture, transportation, and illegal sale of controlled dangerous substances. During the course of these interviews, I have inquired and learned how individuals involved in drug distribution schemes and networks use and disperse the illegal proceeds generated from the illegal sale of controlled dangerous substances, including but not limited to chemicals commonly utilized in the illegal manufacture of methamphetamine.

5. Based on my training, education, and experience, I have become familiar with the manner in which drug traffickers coordinate illegal activity, conduct illegal activity, and the communication methods used to conduct illegal activity. I have learned the following:

a. Drug distributors/traffickers commonly maintain books, records, receipts, notes, ledgers, and other documents/papers both electronically and in paper form, which relate to the transportation, ordering, sale, and distribution of controlled substances, even though such documents may be in code and/or identify customers/sources/co-conspirators through monikers/nicknames. Documentation such as this oftentimes results because drug distributors/traffickers commonly "front" drugs (provide controlled substances on consignment) to their clients and must account for these transactions in order to collect outstanding drug debts.

b. Drug distributors/traffickers commonly maintain addresses or telephone numbers in notebooks, papers, cellular phones, computers and electronic storage media which reflect names, address, and/or telephone numbers for their associates in the drug distribution/trafficking organization, even if said items may be in code, and such traffickers send and receive items listed in this affidavit by mail and other common carriers.

c. Drug users, distributors and traffickers frequently take, or cause to be taken photographs or videotapes of themselves, their associates, their property/assets, and their product, and these individuals usually maintain these photographs or recordings/videos in the residences under their control. These photographs and videos are also often found in the individual's cellular telephone, computers and other electronic storage media.

d. I have participated in numerous searches of cellular telephones found to be in the possession of drug users/dealers/traffickers where text messages were discovered discussing topics such as quantities, prices and the quality of controlled dangerous substances, as well as dates, times and locations for drug transactions are discussed. Almost always, these communications are in coded drug talk/jargon and require review by peace officers experienced in deciphering such communications.

e. In my experience in searching cellular telephones possessed by known drug users/distributors/traffickers, photos and/or videos have been discovered

which evidence the use and distribution of controlled dangerous substances and the proceeds intended for or derived therefrom. Commonly said evidence depicts pictures/videos of drugs for evidencing the respective drugs quality, condition or quantity. Moreover, users will commonly document episodes of drug use in social settings. Additionally, drug distributors will take pictures ("trophy" pictures) or otherwise capture digital recordings for the purpose of memorializing their credibility/capability as a drug dealer and accomplishments (acquisition of assets/large amounts of U.S. currency) relating thereto.

f. In all phases of drug distribution, the utilization of cellular telephones is essential. Drug users/dealers/traffickers use cellular telephones to place calls, as well as communicate by SMS text messaging. As drug dealing necessarily entails constant communications with accomplices, co-conspirators, clients, and sources, these communications virtually always take place by voice calls and text messaging over cellular telephones.

g. Cellular telephones are almost always used by drug distributors as a way to communicate. They will communicate by verbal conversations, digital text messaging, and/or sending photographs to one another. To avoid detection, drug distributors will often times speak in coded language or through use of vague messages. Sometimes the cellular telephone numbers they use are listed in different individuals' name or they will frequently change phone numbers. Drug distributors will often "drop" or switch cellular phones to avoid detection by law enforcement. This will result in the accumulation of several different cellular phones.

BACKGROUND INFORMATION

6. Cellular telephones are often used to facilitate offenses and allow criminals to maintain communication with each other before, during and after the commission of offenses. I am aware that cellular telephones have the capacity to store a vast amount of information, including but not limited to: telephone numbers, voice messages, text messages, e-mail, photographs, videos, address books, records, phone call histories, contact and other information. This information may be contained on the actual cellular

telephone. This data and information is oftentimes also maintained by the various service providers on separate equipment.

7. As such, I am seeking court authority to search individual cell phones described herein as well as court orders directing specific service providers to provide additional information and potentially stored wired and electronic information. This affidavit is made in support of requests to the court for warrants and/or orders to inspect, review and retrieve various information including but not limited to cell tower information, records, stored wired and electronic communications, photographic images and other information more further described herein relating to cellular telephones believed to have been used in the commission of various federal offenses.

8. The request for issuance of a search warrant is made for the seizure of physical evidence regarding federal criminal offenses, any and all information and or data stored in the referenced cellular telephone, to include but not be limited to: the telephone number of the referenced cellular telephone(s), direct connect push-to-talk number of the referenced cellular telephone(s), telephone numbers calling the referenced telephone(s), calls made, received and missed, telephone numbers called by the referenced telephone(s), address and phone books stored within the referenced cellular telephone(s), and any text messages sent, received, saved and found in the referenced telephone(s), voice mails made, received, and saved, calendars, stored photos and digital records, web site visits history, as well as all other stored electronic data and information. (See Attachments A and B).

9. Service providers maintain additional information including electronic records that detail the "cell towers" or "cell sites" accessed by the aforementioned cellular telephones when the devices were used to receive calls, make calls, send text messages, etc. This information will provide data and evidence of the physical movement of the devices and/or their users.

10. Information contained in this Affidavit is based upon my personal knowledge and also from discussions I have had with other law enforcement officers who have investigated these offenses. I have not included each and every fact I know concerning this investigation. However, I have set forth the facts that I believe are essential to establish the necessary foundation and probable cause to support the Search Warrant.

CASE BACKGROUND

11. On October 14, 2020, the Tulsa Police Department's Special Investigations Division (TPD/SID) Narcotics Unit and members of the Drug Enforcement Administration (DEA) Tulsa Resident Office (TRO) executed search warrants in the Tulsa area at three separate residences (4702 S. 91st East Avenue, Tulsa, Oklahoma, 3514 East 32 Street North, Tulsa, Oklahoma and 3210 South 116th East Avenue, Tulsa, Oklahoma). Pedro Santiago Cabrera and Rolando Rena Reyes were located and detained at 4702 South 91st East Avenue in Tulsa, Oklahoma. Two other individuals were present, but were interviewed and released with their personal property.

12. An active methamphetamine conversion lab was present at the residence located at 3514 East 32nd Street North in Tulsa, Oklahoma. Investigators discovered

approximately 25 pounds of crystal methamphetamine and approximately 25 gallons totaling 200 pounds of liquid contained in five-gallon buckets of paint and Rubbermaid containers. The liquid within these containers and the crystal substance located in the residence field-tested positive for methamphetamine.

13. While at 4702 S. 91st East Avenue, investigators advised Pedro Santiago Cabrera of his *Miranda* Rights. After Cabrera waved his *Miranda* Rights, Cabrera stated that he frequents the residence at 3514 East 32nd Street North, Tulsa, Oklahoma to convert liquid methamphetamine to crystal methamphetamine. Cabrera stated he was at the residence as recently as a week ago.

14. While at 4702 S. 91st East Avenue, investigators advised Rolando Rena Reyes of his *Miranda* Rights. After Rene Reyes waived his *Miranda* Rights, he stated that he has seen methamphetamine inside the house, but he is not involved in converting the liquid methamphetamine into the crystal methamphetamine. Rene Reyes stated he is being paid to clean the equipment used to convert the liquid methamphetamine into the crystal methamphetamine once the process has been completed. Rena Reyes stated he had been to 3514 East 32nd Street North, Tulsa, Oklahoma as recent as yesterday (October 13, 2020).

15. While searching the residence at 4702 S. 91st E. Avenue investigators located at black Samsung phone (IMEI # 354142110521996) in the southeast bedroom, believed to be Cabrera's, and a blue and black ZTE cell phone (IMEI # 866728045898532) located in the kitchen of the residence that investigators believe belongs to Reyes.

CELLULAR TELEPHONES & ELECTRONIC DEVICES

During a search of 4702 S. 91st E. Avenue investigators located at black Samsung phone (IMEI # 354142110521996) in the southeast bedroom and a blue and black ZTE cell phone (IMEI # 866728045898532) in the kitchen of the residence. The aforementioned cellular phones are currently in the custody of the Tulsa Police Department, in the Northern District of Oklahoma. The cellular phones are identified as:

a. Samsung phone in an Otter Box case black in color, IMEI # 354142110521996
b. Blue ZTE Cellular telephone IMEI # 866728045898532

The applied-for warrant would authorize the forensic examination of the aforementioned devices for the purpose of identifying electronically stored data particularly described in Attachment B.

Based on the above information, I believe there is probable cause to believe that the phones described herein were used to communicate during and after and to facilitate the commission of drug trafficking activity, in violation of Title 21, United States Code, Section 846 (Conspiracy) and Title 21, United States Code, Section 841(a)(1) (Possession with intent to distribute and distribution of Methamphetamine). Therefore, I respectfully request a warrant and/or the appropriate Orders be issued for the search of the cellular phone and phone records associated with the above referenced phone.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been

viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. There is probable cause to believe that things that were once stored on the device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that smartphone files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a smartphone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the smartphone may retain a log or record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, electronic storage media may contain electronic evidence of how a device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic

evidence that establishes how the devices were used, the purpose of their use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Device file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium is a dynamic process. Whether data stored on a device is evidence may depend on other information stored on the computer and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is, or is not, present on a storage medium.

f. I know that when an individual uses an electronic device as a communication device or a device to obtain information from the Internet related to a criminal act, the individual's electronic device will generally

serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Respectfully submitted,

William Mackenzie
Task Force Officer DEA

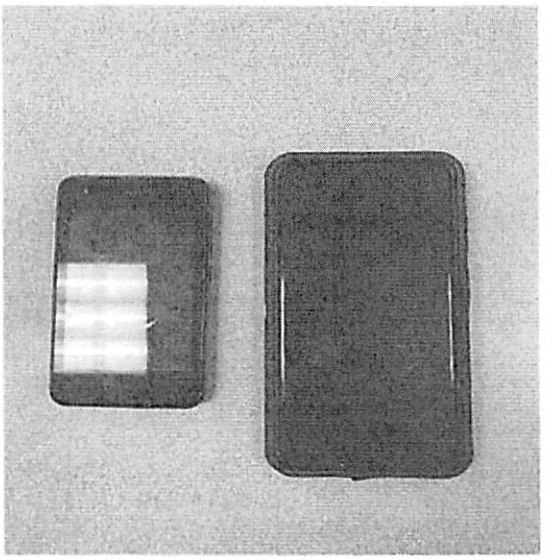
by phone on 20

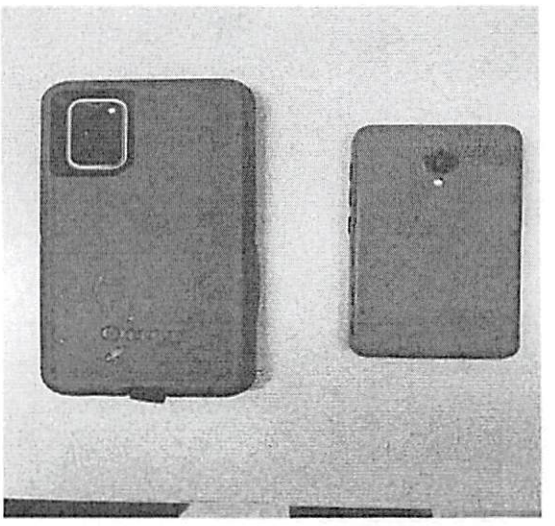
Subscribed and sworn ~~before me on this~~ 20th day of October 2020.

Jodi F. Jayne
United States Magistrate
Northern District of Oklahoma

ATTACHMENT A

1. Black Samsung Cell Phone IMEI # 354142110521996
2. Blue ZTE Cell Phone IMEI # 866728045898532





ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Title 21, United States Code, Section 846 (Conspiracy) and Title 21, United States Code, Section 841(a)(1) (Possession with intent to distribute and distribution of Methamphetamine).

a. records relating to communication with others as to the criminal offense above; including incoming and outgoing voice messages; text messages; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;

b. records relating to documentation or memorialization of the criminal offense above, including voice memos, photographs, videos, and other audio and video media, and all ExIF information and metadata attached thereto including device information, geotagging information, and information of the relevant dates to the media;

c. records relating to the planning and execution of the criminal offense above, including Internet activity, including firewall logs, caches, browser history, and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;

d. application data relating to the criminal offense above;

e. lists of customers and related identifying information;

f. types, amounts, and prices of drug trafficked as well as dates, places, and amounts of specific transactions; and

g. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

2. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;

3. All records and information related to the geolocation of the devices at a specific point in time;

4. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the statutes listed in Paragraph 1 of this Attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.